EP 1274744 (C)

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
21 novembre 2002 (21.11.2002)

PCT

(10) Numéro de publication internationale
WO 02/093332 A1

(51) Classification internationale des brevets[7] : G06F 1/00, G07F 7/10

(21) Numéro de la demande internationale :
PCT/FR02/01433

(22) Date de dépôt international : 25 avril 2002 (25.04.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0/106318 14 mai 2001 (14.05.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gemenos, F-13420 GEMENOS (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **AGOYAN, Michel** [FR/FR]; 193 Chemin des Sables Jaunes, F-13012 Marseille (FR). **FERMY, Alain** [FR/FR]; La Malounière, Bâtiment H, F-13400 Aubagne (FR). **PRADEN, Anne-Marie** [FR/FR]; 4 Lotissement les Chemins d'Aix, F-13122 Ventabren (FR).

(74) Mandataire : **BRUN, Philippe**; c/o Gemplus, Service brevets, BP 100, F-13881 Gemenos Cedex (FR).

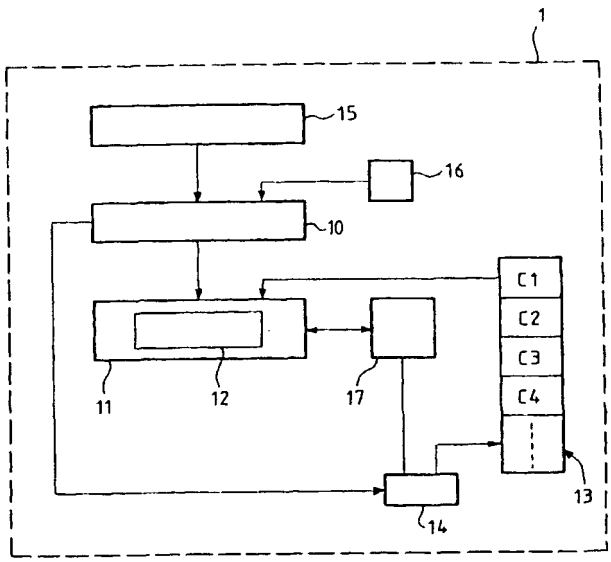
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) **Title:** METHOD FOR PROTECTING A LOGIC CIRCUIT FROM EXTERNAL ATTACKS, AND LOGIC UNIT COMPRISING A LOGIC CIRCUIT TO BE PROTECTED AGAINST EXTERNAL ATTACKS

(54) **Titre :** PROCEDE DE PROTECTION D'UN CIRCUIT LOGIQUE CONTRE DES ATTAQUES EXTERIEURES, ET UNITE LOGIQUE COMPRENANT UN CIRCUIT LOGIQUE A PROTEGER CONTRE DES ATTAQUES EXTERIEURES



(57) Abstract: The invention concerns a method for protecting a logic circuit (11) contained in a logic unit (1) against attacks external to said unit. Said method comprises the following operations: generating in the unit (1) a programming instruction of a programmable logic circuit (12) comprised in the logic circuit (11); loading in the programmable logic circuit (12) in response to the programming instruction, a specific programming configuration (C1) selected among a plurality of configurations different from one another (C1, , C4); programming the programmable logic circuit (12) in accordance with the specific configuration (C1).

(57) Abrégé : La présente invention concerne un procédé de protection d'un circuit logique (11) contenu dans une unité logique (1) contre des attaques extérieures à cette unité. Ce procédé comprend les opérations suivantes : génération au sein de l'unité (1) d'une instruction de programmation d'un circuit logique programmable (12) contenu dans le circuit logique (11); chargement au sein du circuit logique programmable (12), en réponse à l'instruction de programmation, d'une configuration de programmation spécifique (C1) choisie parmi une pluralité de configurations de programmation distinctes les unes des autres (C1, ..., C4); programmation du circuit logique programmable (12) selon la configuration spécifique (C1).

WO 02/093332 A1

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE DE PROTECTION D'UN CIRCUIT LOGIQUE CONTRE DES ATTAQUES EXTERIEURES, ET UNITE LOGIQUE CONTENANT UN CIRCUIT LOGIQUE A PROTEGER CONTRE DES ATTAQUES EXTERIEURES

La présente invention concerne un procédé de protection d'un circuit logique, et par exemple d'un processeur contre des attaques extérieures. Elle s'applique notamment, mais non exclusivement, aux microprocesseurs se trouvant dans les puces des cartes à puce. La présente invention concerne également une unité logique contenant un circuit logique à protéger contre des attaques extérieures, se trouvant par exemple au sein de la puce d'une carte à puce.

De manière connue, le microprocesseur incorporé dans la puce d'une carte à puce utilise lors de son fonctionnement un certain nombre de programmes. Dans ce fonctionnement, il utilise des données provenant par exemple de l'extérieur, et des données se trouvant dans la mémoire de la carte. Certaines de ces données peuvent être des données confidentielles ; c'est le cas notamment du code secret de la carte. Or, durant l'exécution d'un programme par le microprocesseur, ces données circulent sur des bus et sont donc plus aisément détectables.

Afin de protéger ces données, on peut utiliser différentes méthodes de protection. L'une de ces méthodes connues, appelée « scrambling de bus » repose sur le chiffrage des données qui circulent sur les bus, ce qui assure un brouillage de bus et donc une protection supplémentaire de ces dernières.

Cependant, une telle méthode est encore vulnérable. En effet, le microprocesseur et les circuits logiques contenus dans la puce sont constitués de circuits monolithiques dont les fonctionnalités sont figées une

fois pour toutes en sortie de fabrication. Ces circuits monolithiques comprennent des cellules logiques, telles que des portes, des bascules, des entrées-sorties, etc..., et des connexions reliant ces cellules, ces connexions étant donc figées en sortie d'usine. Par conséquent, la puissance consommée par ces circuits lors de chaque utilisation (c'est-à-dire lors de chaque exécution d'une instruction) ne dépend que des données échangées entre les différentes cellules.

Ainsi, pour détecter ces données, il suffit de solliciter le circuit au moyen d'un message d'instruction puis d'effectuer une analyse de la puissance consommée lors de l'exécution de cette instruction par le circuit. En répétant plusieurs fois cette opération et en corrélant les données obtenues à chaque fois, on augmente la quantité d'information concernant une donnée observée et l'on finit par la reconstituer. Une telle méthode de détection est connue sous le nom de Simple Power Analysis ou Differential Power Analysis, et décrite notamment dans le document WO 99/63693.

Les données contenues dans la mémoire de la carte, et plus particulièrement les données confidentielles, doivent donc être protégées de manière plus efficace contre des attaques extérieures visant à les récupérer pour ensuite utiliser la carte de manière frauduleuse.

Par ailleurs, l'analyse microscopique d'un circuit logique à partir de celle des bus de connexion de ce dernier, facilement reconnaissables sur le silicium, conduit à la détection du fonctionnement logique de ce circuit, et permet notamment de le copier plus facilement. Même si des techniques de brouillage de bus sont utilisées pour empêcher ce genre d'analyses, appelées aussi attaques invasives, elles ne sont pas assez efficaces.

La présente invention a donc pour but de mettre au point un procédé de protection d'un circuit logique contre des attaques extérieures, qui assure une protection plus efficaces que ceux de l'art antérieur contre les attaques par analyse de consommation ou les attaques invasives.

La présente invention propose à cet effet un procédé de protection d'un circuit logique contenu dans une unité logique contre des attaques extérieures à ladite unité, ledit procédé comprenant les opérations suivantes :

- génération au sein de ladite unité d'une instruction de programmation d'un circuit logique programmable contenu dans ledit circuit logique
- chargement au sein dudit circuit logique programmable, en réponse à ladite instruction de programmation, d'une configuration de programmation spécifique choisie parmi une pluralité de configurations de programmation distinctes les unes des autres
- programmation dudit circuit logique programmable selon ladite configuration spécifique.

Un circuit logique programmable est un circuit intégré qui n'a pas de fonctionnalité figée en sortie de fabrication. C'est seulement après la fabrication, lors d'une phase de programmation, que ce circuit prend sa fonctionnalité. Cette programmation peut, de manière générale pour les circuits logiques programmables, être effectuée dans un programmateur, ou, comme c'est le cas selon la présente invention, « in situ ». Cette programmation modifie les connexions reliant les cellules logiques du circuit entre elles.

Les circuits logiques programmables rendant possible ce type de programmation (« in situ ») par chargement depuis l'extérieur du circuit sont notamment les circuits logiques programmables utilisant la technologie de programmation SRAM (Static Random Access Memory).

Selon l'invention, pour protéger un circuit logique contre des attaques extérieures telles que celles décrites plus haut, on incorpore à ce dernier un circuit logique programmable. Une instruction de programmation du circuit logique programmable est générée et envoyée à ce dernier, de sorte qu'il va chercher une configuration de programmation parmi un certain nombre de configurations de programmation possibles, par exemple

embarquées au sein d'une carte à puce, et se pogramme selon cette configuration.

On appelle configuration de programmation dans le cadre de la présente invention la programmation des cellules logiques (fonctions logiques simples, multiplexeurs, bascules, entrées-sorties, etc...) du circuit logique programmable, afin de leur donner une fonctionnalité, ainsi que celle de la matrice d'interconnexion entre ces cellules.

Ainsi, selon l'invention, le circuit logique à protéger comporte au moins une partie qui n'est pas programmée à l'avance, c'est-à-dire qui n'est donc pas figée à l'avance, et se programme selon une configuration donnée, embarquée. La configuration et le profil de puissance du circuit programmable changent donc régulièrement.

Lors d'une tentative d'attaque extérieure par analyse de la puissance consommée, cette dernière, qui dépend de la configuration du circuit logique, pourra donc être différente à chaque fois. Ainsi, on rend beaucoup plus difficile et longue la recherche des informations confidentielles contenues dans une carte contenant un tel circuit logique.

Par ailleurs, lorsque le circuit est au repos, c'est-à-dire qu'il n'est pas alimenté, sa partie circuit logique programmable se comporte comme une boîte noire (les cellules logiques ne sont pas reliées entre elles), de sorte qu'aucune attaque invasive n'est possible. En effet, il n'est alors pas possible, par simple analyse des circuits connectés aux bus, de retrouver les fonctions logiques du circuit.

Selon un mode de réalisation de l'invention, l'opération de génération d'une instruction de programmation peut être effectuée à des instants définis par l'unité logique, par exemple de manière périodique suivant un signal d'horloge (provenant par exemple d'une horloge de l'unité logique), ou de manière aléatoire ou quasi-aléatoire (en utilisant par exemple une focntion Random ou Pseudo-Random), ou encore à chaque mise sous tension du circuit logique à protéger. Ainsi, la génération des instructions de

programmation est décidée de manière autonome par l'unité logique, et n'est pas programmée de l'extérieur, ce qui rend les attaques encore plus difficiles.

En outre, l'unité logique peut être programmée de sorte que le procédé selon l'invention est mis en œuvre lors de chaque réception d'une instruction devant mettre en œuvre le circuit logique à protéger, et avant que ce dernier ne soit activé. Ainsi, à chaque utilisation du circuit logique, consécutive à la réception d'une instruction extérieure, la puissance consommée par ce circuit logique est différente, son implémentation logique étant différente, et une protection du circuit logique contre une attaque par analyse de la puissance consommée est ainsi réalisée.

De manière avantageuse, le choix de la configuration de programmation spécifique parmi les configurations configurations possibles peut être effectué de manière aléatoire lors de chaque mise en œuvre du procédé selon l'invention. On accroît ainsi la protection du circuit logique.

La présente invention concerne également une unité logique comprenant :

- un processeur
- un circuit logique protégé contre des attaques extérieures à ladite unité
- une mémoire

caractérisée en ce que ledit circuit logique comprend un circuit logique programmable contenant des cellules logiques et des connexions reliant lesdites cellules logiques, en ce que ladite mémoire contient une pluralité de configurations possibles pour ledit circuit logique programmable, et en ce que ladite unité comprend également des moyens pour générer des instructions de programmation dudit circuit logique programmable.

Une telle unité permet de mettre en œuvre le procédé selon l'invention énoncé ci-dessus.

Selon l'invention, cette unité peut en outre comprendre un générateur de nombres aléatoires, qui accroît la protection puisque chaque

configuration est alors choisie de manière aléatoire et donc très difficilement prédictible.

Le circuit logique à protéger peut être contenu notamment dans le processeur de cette unité. On protège ainsi de manière accrue certaines fonctions du processeur. Le circuit logique à protéger peut également être contenu au sein d'un dispositif de sécurisation déjà présent au sein de l'unité logique, comme par exemple un crypto-coprocesseur.

De manière avantageuse, le circuit logique programmable est un FPGA (Field Programmable Gate Array).

Selon l'invention, le circuit logique programmable utilisé peut également être re-programmable. Ceci permet de modifier sa configuration lors de chaque exécution d'une instruction extérieure. Dans ce cas, on choisit par exemple un circuit logique programmable à EPROM (Erasable Programmable Read Only Memory) et/ou à SRAM.

Une application possible de l'invention se situe dans le domaine des cartes à puce. Ainsi, une unité selon l'invention peut être contenue dans la puce d'une telle carte.

D'autres caractéristiques et avantages de l'invention apparaîtront dans la description ci-après d'un mode de réalisation de l'invention, donné à titre illustratif et nullement limitatif.

La figure unique représente de manière schématique une carte à puce contenant un dispositif de protection fonctionnant selon le procédé de l'invention.

On voit dans cette figure une unité logique sous forme de puce 1 pour carte à puce, comprenant :

- un microprocesseur 10,
- un circuit logique 11 à protéger, contenant un circuit logique programmable 12, tel qu'un FPGA (Field Programmable Gate Array) par exemple,

- une mémoire 13 contenant notamment une pluralité de configurations possibles C1 à C4 pour le circuit logique programmable 12
- un générateur 14 de nombres aléatoires (qui génère de manière aléatoire un index de configuration)
- une interface 15 de la carte 1 avec l'extérieur
- un circuit d'horloge 16.

Le circuit logique 11 à protéger peut être tout circuit de la carte, et par exemple tout ou partie d'un crypto-coprocesseur (tel que celui décrit dans le document mentionné plus haut), le microprocesseur lui-même ou tout autre circuit que l'on souhaite protéger contre des attaques extérieures.

Un circuit FPGA 12 utilisé dans le mode de réalisation présenté sur la figure en tant circuit logique programmable comprend, de manière connue et non représentée, une pluralité de cellules logiques telles que des portes, des bascules, des entrées-sorties, etc... et des connexions reliant entre elles ces cellules logiques. De tels circuits sont classiques et commercialisés à l'heure actuelle par de nombreuses sociétés.

Le FPGA 12 est re-programmable.

On explique à présent le fonctionnement de la carte à puce 1 et la manière avec laquelle le circuit logique 11 à protéger est protégé selon l'invention.

De manière périodique, en fonction notamment du signal d'horloge émis par le circuit d'horloge 16, le microprocesseur 10 génère une instruction de programmation du FPGA 12. Cette instruction de programmation est envoyée au FPGA 12 et en même temps au générateur de nombres aléatoires 14. Ce dernier pointe alors, selon le nombre aléatoire généré, sur l'une des configurations C1 à C4, par exemple sur la configuration C1.

Le FPGA 12 va ensuite (ou en parallèle) chercher sa configuration au sein de la mémoire 13, en suivant le pointage généré par le générateur de nombres aléatoires 14. Dans l'exemple choisi, le FPGA 12 reçoit donc l'instruction de se configurer selon la configuration C1, et exécute cette

instruction de sorte que ses cellules logiques sont maintenant reliées et programmées selon la configuration C1.

Dans cet exemple, on a décrit la génération par le microprocesseur 10 d'une instruction de programmation du FPGA 12 de manière périodique en fonction d'un signal d'horloge. Ceci permet au FPGA 12 d'être reprogrammé par « décision » interne à la puce, sans l'intervention d'aucune instruction extérieure de programmation, et rend donc le procédé selon l'invention très efficace.

Le même résultat peut être obtenu en programmant par exemple à l'avance le microprocesseur 10 pour qu'il génère des instructions de programmation du FPGA 12 à des instants prédéfinis, ou à des instants aléatoires ou quasi-aléatoires. On peut aussi prévoir que chaque mise sous tension du microprocesseur 10 entraîne la génération par ce dernier d'une instruction de programmation du FPGA 12.

Par ailleurs, on peut encore prévoir que lorsqu'une instruction provenant de l'extérieur de la carte à puce 1 est transmise à cette dernière par l'intermédiaire de l'interface 15 et doit être exécutée par le circuit logique 11, le microprocesseur 10 génère aussi une instruction de programmation du FPGA 12 et le procédé selon l'invention est mis en œuvre avant que l'instruction provenant de l'extérieur de la carte soit exécutée.

Lorsqu'une autre instruction destinée à être exécutée par la carte 1 est transmise à cette dernière par l'intermédiaire de l'interface 15, le procédé ci-dessus se reproduit, et ainsi de suite.

Grâce à l'utilisation du générateur de nombre aléatoires 14, la configuration du FPGA 12 change de manière aléatoire lors de chaque instruction à exécuter par le circuit logique 11.

De la même manière, le circuit d'horloge peut envoyer directement au FPGA 12 et au générateur de nombres aléatoires 14 une instruction de programmation, soit de façon périodique (en fonction par exemple de la fin de comptage d'un timer), soit en fonction de la détection d'une situation

particulière dans le circuit 11 à partir de l'état de signaux internes, soit en fonction d'un reset, soit encore en fonction de la réception d'une commande particulière venue de l'extérieur.

Ainsi, comme expliqué plus haut, des attaques extérieures par analyse de la consommation du circuit logique 11 sont rendues très difficiles du fait du changement quasiment non prédictible de la configuration du FPGA 12 que contient ce dernier.

Par ailleurs, il est à noter que lorsque le FPGA 12 n'est pas sous tension, c'est-à-dire lorsqu'il n'est sollicité par aucune instruction extérieure, les connexions entre ses cellules logiques sont inexistantes, de sorte qu'il apparaît comme une boîte noire (on dit aussi « mer de portes ») et rend donc impossibles les attaques invasives. Il doit alors être reprogrammé lors de chaque mise sous tension. C'est le cas notamment lorsque la technologie SRAM est utilisée dans le FPGA.

Bien entendu, le mode de réalisation qui vient d'être décrit ne constitue qu'un exemple d'application du procédé selon l'invention, et l'on pourra remplacer tout moyen par un moyen équivalent sans sortir du cadre de l'invention.

Notamment, on pourra remplacer le générateur de nombres aléatoires par une programmation prédéfinie de la suite des configurations que le circuit logique programmable doit adopter.

Par ailleurs, les instructions de programmation envoyées au circuit logique programmable peuvent provenir du microprocesseur, ou d'une fonction logique embarquée dans la carte, dite générateur d'instructions de programmation 17, détectant une information circulant dans la carte et agissant de manière autonome.

Le circuit logique programmable selon l'invention peut être incorporé dans toute zone sensible de la carte, que l'on veut protéger.

Enfin, le circuit logique programmable utilisé selon l'invention peut être choisi parmi tout type de circuit logique programmable connu, comme

notamment les CPLD (Complex Programmable Logic Device), SPLD (Simple Programmable Logic Device), PLA (Programmable Logic Array).

Tout autre type de circuit logique programmable que ceux mentionnés ci-dessus peut également être utilisé dans le cadre de l'invention.

Enfin, on pourra remplacer tout moyen par un moyen équivalent sans sortir du cadre de l'invention.

REVENDICATIONS

1. Procédé de protection d'un circuit logique (11) contenu dans une unité logique (1) contre des attaques extérieures à ladite unité, ledit procédé comprenant les opérations suivantes :
   - génération au sein de ladite unité (1) d'une instruction de programmation d'un circuit logique programmable (12) contenu dans ledit circuit logique (11)
   - chargement au sein dudit circuit logique programmable (12), en réponse à ladite instruction de programmation, d'une configuration de programmation spécifique (C1) choisie parmi une pluralité de configurations de programmation distinctes les unes des autres (C1, ..., C4)
   - programmation dudit circuit logique programmable (12) selon ladite configuration spécifique (C1).

2. Procédé selon la revendication 1 caractérisé en ce que l'opération de génération d'une instruction de programmation est effectuée à des instants définis par ladite unité logique (1).

3. Procédé selon la revendication 2 caractérisé en ce que l'opération de génération d'une instruction de programmation est effectuée de manière périodique ou de manière aléatoire ou quasi-aléatoire, ou encore à chaque mise sous tension dudit circuit logique.

4. Procédé selon l'une des revendications 1 à 3 caractérisé en ce qu'il est effectué lors de chaque réception par ledit circuit logique (11) d'une instruction extérieure audit circuit logique (11) à exécuter par ledit circuit logique (11), avant l'exécution de ladite instruction extérieure.

5. Procédé selon l'une des revendications 1 à 4 caractérisé en ce que le choix de ladite configuration spécifique est effectué de manière aléatoire lors de chaque mise en œuvre dudit procédé.

6. Unité logique (1) comprenant :

- un processeur (10)
- un circuit logique (11) protégé contre des attaques extérieures à ladite unité (1)
- une mémoire (13)

caractérisée en ce que ledit circuit logique (11) comprend un circuit logique programmable (12) contenant des cellules logiques et des connexions reliant lesdites cellules logiques, en ce que ladite mémoire (13) contient une pluralité de configurations possibles (C1, ..., C4) pour ledit circuit logique programmable (12), et en ce que ladite unité (1) comprend également des moyens (10, 16, 17) pour générer des instructions de programmation dudit circuit logique programmable (12).

7. Unité selon la revendication 6 caractérisée en ce qu'elle comprend en outre un générateur de nombres aléatoires (14).

8. Unité selon l'une des revendications 6 ou 7 caractérisée en ce que ledit circuit logique (11) est contenu dans ledit processeur (10).

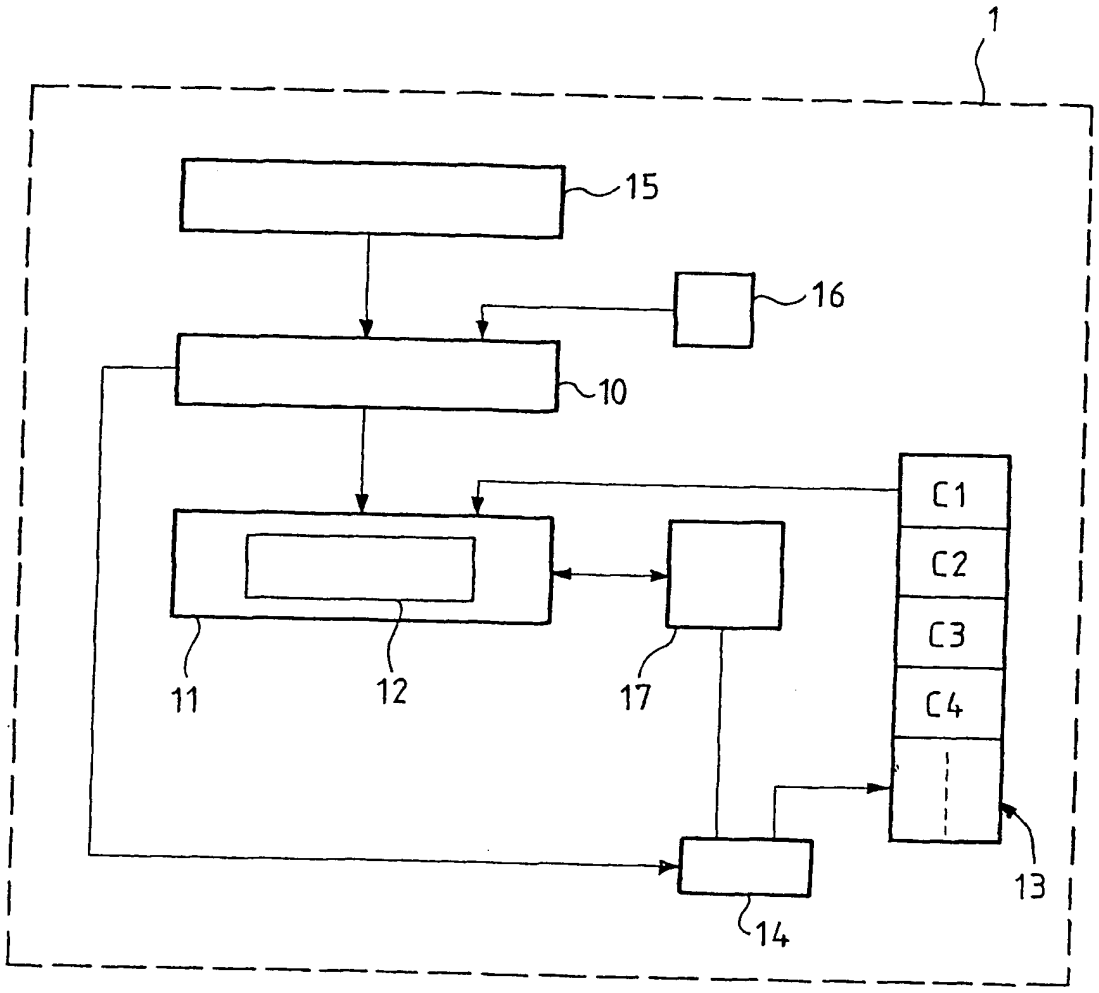
9. Unité selon l'une des revendications 6 à 8 caractérisée en ce que ledit circuit logique programmable (12) est un FPGA (Field Programmable Gate Array).

10. Unité selon la revendication 9 caractérisée en ce que ledit FPGA est du type à EPROM et/ou à SRAM.

11. Unité selon l'une des revendications 6 à 10 caractérisé en ce que ledit circuit logique programmable (12) est re-programmable.

12. Unité selon l'une des revendications 6 à 11 caractérisée en ce que ledit générateur d'instructions de programmation est ledit processeur (10).

13. Unité selon l'une des revendications 6 à 12 caractérisée en ce qu'elle appartient à la puce d'une carte à puce.



INTERNATIONAL SEARCH REPORT

	National Application No PCT/FR 02/01433

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 08542 A (KONINKL PHILIPS ELECTRONICS NV) 17 February 2000 (2000-02-17) abstract page 2, line 5 -page 3, line 9 page 6, line 19 -page 7, line 7 page 8, line 13 -page 9, line 2 figure 1	1,6,7,13
A	FR 2 776 410 A (GEMPLUS CARD INT) 24 September 1999 (1999-09-24) abstract page 3, line 25 -page 5, line 9 figure 1	1,2,6,7, 13

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 August 2002	08/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 02/01433

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 977 108 A (PHILIPS CORP INTELLECTUAL PTY ;KONINKL PHILIPS ELECTRONICS NV (NL)) 2 February 2000 (2000-02-02) column 1, line 3 - line 27 column 4, line 18 -column 5, line 14 figure 1 -----	1,6,7,13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

ational Application No
PCT/FR 02/01433

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0008542	A	17-02-2000	CN	1286768 T	07-03-2001
			WO	0008542 A1	17-02-2000
			EP	1040402 A1	04-10-2000
FR 2776410	A	24-09-1999	FR	2776410 A1	24-09-1999
			CA	2323006 A1	30-09-1999
			CN	1288548 T	21-03-2001
			EP	1062633 A1	27-12-2000
			WO	9949416 A1	30-09-1999
			JP	2002508549 T	19-03-2002
EP 0977108	A	02-02-2000	DE	19834076 A1	10-02-2000
			CN	1253331 A	17-05-2000
			EP	0977108 A2	02-02-2000
			JP	2000122932 A	28-04-2000

RAPPORT DE RECHERCHE INTERNATIONALE

nde Internationale No
PCT/FR 02/01433

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F1/00 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Categorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 00 08542 A (KONINKL PHILIPS ELECTRONICS NV) 17 février 2000 (2000-02-17) abrégé page 2, ligne 5 -page 3, ligne 9 page 6, ligne 19 -page 7, ligne 7 page 8, ligne 13 -page 9, ligne 2 figure 1 ---	1,6,7,13
A	FR 2 776 410 A (GEMPLUS CARD INT) 24 septembre 1999 (1999-09-24) abrégé page 3, ligne 25 -page 5, ligne 9 figure 1 ---	1,2,6,7, 13
	-/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
1 août 2002	08/08/2002

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Arbutina, L

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 02/01433

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 0 977 108 A (PHILIPS CORP INTELLECTUAL PTY ;KONINKL PHILIPS ELECTRONICS NV (NL)) 2 février 2000 (2000-02-02) colonne 1, ligne 3 - ligne 27 colonne 4, ligne 18 -colonne 5, ligne 14 figure 1 -----	1,6,7,13

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 02/01433

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0008542	A	17-02-2000	CN	1286768 T	07-03-2001
			WO	0008542 A1	17-02-2000
			EP	1040402 A1	04-10-2000
FR 2776410	A	24-09-1999	FR	2776410 A1	24-09-1999
			CA	2323006 A1	30-09-1999
			CN	1288548 T	21-03-2001
			EP	1062633 A1	27-12-2000
			WO	9949416 A1	30-09-1999
			JP	2002508549 T	19-03-2002
EP 0977108	A	02-02-2000	DE	19834076 A1	10-02-2000
			CN	1253331 A	17-05-2000
			EP	0977108 A2	02-02-2000
			JP	2000122932 A	28-04-2000